На основу члана 157. став 9. Закона о електронским комуникацијама („Службени гласник РС”, број 35/23) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС, 44/14 и 30/18 – др. закон),

Влада доноси

УРЕДБУ

о утврђивању мера за смањење безбедносних ризика повезаних са увођењем мобилних мрежа пете генерације

"Службени гласник РС", број 17 од 28. фебруара 2025.

Предмет Уредбе

Члан 1.

Овом уредбом се ближе уређују инструменти за смањење безбедносних ризика повезаних са увођењем мобилних мрежа пете генерације који обухватају стратешке, техничке и мере подршке за превазилажење идентификованих безбедносних ризика којима се обезбеђује безбедност, доступност, поверљивост, интегритет и отпорност података, услуга и инфраструктуре 5G мрежа, а које се заснивају на процени изложености безбедносним ризицима које доноси увођење електронских комуникационих мрежа пете генерације.

Значење појединих израза

Члан 2.

Употребљени изрази у Уредби имају следеће значење:

1) 5G мрежа је мрежа пете генерације електронских комуникација (у даљем тексту: 5G мрежа) која представља скуп свих релевантних елемената и функција мрежне инфраструктуре за мобилне и бежичне комуникационе технологије који се користе за повезивање и пружање јавне мобилне и бежичне електронске комуникационе услуге корисницима са напредним карактеристикама, као што су велике брзине преноса података и велики капацитети преноса података, комуникације са малим кашњењем, изузетно висока поузданост или могућност повезивања великог броја уређаја. Она може укључивати постојеће мрежне елементе који се заснивају на претходним генерацијама мобилних и бежичних комуникационих технологија, као што су 4G или 3G, ако се користе за пружање 5G услуга;

2) 5G услуга је електронска комуникациона услуга у чијем пружању се користи 5G мрежа;

3) оператор 5G мреже је правно лице које је уписано у евиденцију привредних субјеката коју води Регулаторно тело за електронске комуникације и поштанске услуге (у даљем тексту: Регулатор) и које намерава да гради или поседује 5G мрежу у сврху пружања јавно доступних електронских комуникационих услуга;

4) добављач 5G опреме је физичко или правно лице које обезбеђује хардвер, софтвер, услуге или подршку неопходну за изградњу, одржавање и функционисање 5G мреже. Ово укључује произвођаче електронске комуникационе опреме, добављаче софтверских решења за управљање мрежом, као и пружаоце услуга управљања мрежом који учествују у одржавању, управљању и надзору 5G инфраструктуре;

5) безбедносни ризик представља потенцијалну рањивост или претњу која може угрозити безбедност, поверљивост, интегритет, отпорност и/или доступност података, услуга или инфраструктуре 5G мрежа;

6) добављач услуга управљања мрежом је субјект који пружа услуге у вези са постављањем, управљањем, радом и одржавањем 5G мреже и њених елемената и функција, путем пружања помоћи или активног управљања које се спроводи у просторијама корисника услуге или на даљину;

7) добављач услуга управљања безбедношћу је пружалац управљаних услуга који спроводи или пружа помоћ у спровођењу активности управљања ризиком у области безбедности 5G мреже и њених елемената и функција.

Обим примене

Члан 3.

Одредбе ове уредбе се односе на:

1) операторе 5G мреже,

2) добављаче 5G опреме.

Одредбе ове уредбе се не односе на субјекте јавне власти који обављају активности у областима националне безбедности, јавне безбедности, националне одбране или спровођења кривичног законодавства и у области електронске управе.

Циљеви

Члан 4.

Инструменти, односно процедуре и мере утврђени овом уредбом имају за циљ:

1) обезбеђење високог нивоа безбедности, доступности, поверљивости, интегритета и отпорности 5G мрежа и кључних компоненти 5G мреже и безбедности у пружању 5G услуга;

2) успостављање јединственог оквира за процену и ублажавање ризика повезаних са успостављањем и радом 5G мрежа и добављачима 5G опреме;

3) јачање сарадње између надлежних органа, оператора и добављача у идентификацији и управљању ризицима који се односе на безбедност, доступност, поверљивост, интегритет и отпорност 5G мрежа;

4) диверзификацију добављача 5G опреме како би се омогућила безбедност, поверљивост доступност и отпорност 5G мрежа и услуга и смањила зависност од појединог добављача;

5) заштиту националне безбедности;

6) усаглашавање са правним оквиром Европске уније, укључујући Препоруку Европске комисије о информационој безбедности 5G мрежа, (*Commission Recommendation Cybersecurity of 5G networks*), ЕУ координисану процену ризика сајбер безбедности 5G мрежа (*EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*) и Сајбер безбедност 5G мрежа: ЕУ алат за мере за ублажавање ризика (*Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*).

Кључне компоненте 5G мреже

Члан 5.

На основу важности појединих компоненти 5G мреже са становишта безбедносних ризика идентификовани су следећи кључни елементи и функције 5G мреже (у даљем тексту: кључне компоненте 5G мреже):

– функције језгра мреже (Core Network) које обухватају аутентификацију корисничке опреме, роминг и управљање комуникационом везом, пренос података корисничке опреме, управљање политикама приступа, регистрацију и ауторизацију мрежних услуга, складиштење података крајњих корисника и мрежних података, повезивање са мобилним мрежама трећих страна, излагање функција језгра мреже спољним апликацијама и распоређивање корисничких уређаја по мрежним слојевима (slices);

– функције виртуализације мреже (Network Function Virtualisation – NFV) и оркестрације мреже (Management and Network Orchestration – MANO);

– системи управљања и услуге подршке (осим MANO) односе се на системе и услуге које управљају и подржавају функционисање мреже, али нису директно повезане са управљањем виртуелизованим ресурсима и обухватају системе за управљање мрежом (Network Management Systems – NMS), системе за управљање перформансама, подршку за операције и бизнис подршку (Operations Support Systems – OSS и Business Support Systems – BSS), системе за безбедносно управљање;

– радио приступна мрежа (Radio Access Network – RAN) која обухвата базне станице за радио приступ;

– транспортне и преносне функције обухватају основне функције које омогућавају пренос података унутар и између различитих делова мреже, укључујући хардверске компоненте као што су рутери, свичеви и опрема за филтрирање (заштитни зидови – firewalls), системи за заштиту од неовлашћеног приступа (IPS)), као и комуникационе протоколе потребне за пренос, који су од кључног значаја за обезбеђивање брзине, капацитета и безбедности комуникације;

– међумрежне тачке размене (Internetwork Exchanges) које омогућавају комуникацију између различитих мрежа и укључују IP мреже ван инфраструктуре мобилних оператора, као и мрежне услуге које пружају треће стране.

Министарство надлежно за област електронских комуникација (у даљем тексту: Министарство) може, у оквиру националне процене ризика, да одреди и друге елементе и функције као кључне компоненте 5G мреже.

Министарство може да, на основу свеобухватне анализе демографских, економских, друштвених и националних безбедносних фактора, дефинише одређена географска подручја као подручја са посебном осетљивошћу.

Министарство, у оквиру националне анализе ризика, утврђује степен осетљивости сваке кључне компоненте 5G мреже на потенцијалне претње и рањивости узимајући у обзир утицај на поверљивост, доступност, безбедност, интегритет и/или отпорност 5G мреже, као и обим утицаја у смислу броја корисника, трајања, броја базних станица или ћелија које су погођене, осетљивости информација које су измењене или којима се приступило као и друге утицаје. Степен осетљивости може бити означен као критичан, висок и умерен.

Мрежни оперативни центар мобилног оператора (Network Operations Centre – NOC) и Безбедносни оперативни центар мобилног оператора (Security Operations Centre – SOC) морају бити лоцирани на територији Републике Србије.

Национална процена ризика 5G мрежа и услуга

Члан 6.

Министарство спроводи свеобухватну националну процену ризика 5G мрежа и услуга (у даљем тексту: национална процена ризика) најмање једном у периоду од две године.

Национална процена ризика нарочито садржи:

– идентификовање кључних компоненти 5G мреже и степена њихове осетљивости на безбедносне ризике;

– процену претњи при чему се анализирају потенцијалне претње, физички ризици, људске грешке и други фактори који могу угрозити безбедност, отпорност, доступност, интегритет и поверљивост 5G мрежа и услуга;

– процену рањивости при чему се оцењују слабости у технолошким решењима, опреми, софтверу, процесима, интерним процедурама и људским ресурсима;

– анализу и категоризацију безбедносних ризика 5G мрежа и услуга на основу комбинације вероватноће настанка ризика са потенцијалним утицајем на безбедност, отпорност, доступност и поверљивост 5G мреже;

– процену ризика добављача 5G опреме на основу утврђених критеријума;

– анализу степена диверзификације добављача 5G опреме на нивоу кључних компоненти 5G мреже на националном нивоу и на нивоу сваког оператора 5G мреже;

– препоруке за управљање ризицима које обухватају стратешке, техничке и мере подршке како би се безбедносни ризици смањили или елиминисали, као и временски оквир за њихову имплементацију;

– мере и рокове које субјекти из члана 3. став 1. тачка 1. ове уредбе треба да испуне.

Министарство припрема националну процену ризика на основу појединачних процена ризика оператора 5G мрежа у складу са чланом 7. ове уредбе и

добављача 5G опреме у складу са чланом 8. ове уредбе, на основу процене ризика добављача 5G опреме из члана 9. ове уредбе, као и на основу стручних мишљења добијених од других надлежних органа и организација, укључујући Министарство унутрашњих послова, Министарство одбране, Министарство правде, Канцеларију за информационе технологије и електронску управу, Безбедносно-информативну агенцију, Регулатора и Комисију за заштиту конкуренције.

Појединачне процене ризика се достављају Министарству у складу са чланом 7. ст. 1. и 5. и чланом 8. ст. 3 и 4. ове уредбе.

Информације означене одређеним степеном тајности у појединачној процени ризика оператора 5G мреже и добављача 5G опреме се не могу јавно објављивати и користити у друге сврхе осим за потребе израде националне процене ризика.

Уколико се приликом појединачне процене ризика обрађују лични подаци сви видови прикупљања података, врста и обим података, сврха обраде података, садржај података, доступност података, мере њихове заштите и друга питања од значаја за заштиту података о личности морају бити у складу са законом којим се уређује заштита података о личности.

У току израде националне процене ризика Министарство организује редовне консултације са операторима 5G мреже и добављачима 5G опреме.

Приликом израде националне процене ризика Министарство узима у обзир и релевантне најбоље праксе земаља Европске уније и препоруке садржане у Препоруци Европске комисије о информационој безбедности 5G мрежа (*Commission Recommendation Cybersecurity of 5G networks*), ЕУ координисаној процени ризика сајбер безбедности 5G мрежа (*EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*), као и у Сајбер безбедности 5G мрежа: ЕУ алат за мере за ублажавање ризика (*Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*).

Иницијална национална процена ризика се израђује у року од 18 месеци од ступања на снагу ове уредбе, а потом редовно, у складу са роком из става 1. овог члана.

Влада, на предлог Министарства, даје сагласност на националну процену ризика која се објављују на интернет страници Министарства, уз изузимање података који су означени одређеним степеном тајности у складу са законом којим се уређује тајност података, односно који су означени као пословна тајна актом власника податка или уговором, у складу са законом којим се уређује заштита пословне тајне.

Регулатор је надлежан за спровођење мера које произлазе из националне процене ризика и контролу њихове испуњености.

Регулатор, у року од 30 дана од дана објављивања националне процене ризика, покреће поступак по службеној дужности, у складу са прописом којим се уређује општи управни поступак, и доноси решење којим операторима 5G мреже утврђује конкретне мере и рок у коме су они дужни да их испуне.

Решење Регулатора из става 12. овог члана је коначно и против њега се може покренути управни спор.

Процена ризика од стране оператора 5G мреже

Члан 7.

Оператор 5G мреже дужан је да изради сопствену процену ризика 5G мреже и услуга, откривајући рањивости и претње које утичу на њих, у року од шест месеци од почетка рада 5G мреже, односно најкасније у року од девет месеци од ступања на снагу ове уредбе.

Процена ризика оператора из става 1. овог члана обухвата следеће елементе:

– Процену осетљивости сваког елемента и функције 5G мреже који чине кључне компоненте 5G мреже и категоризацију степена осетљивости (критичан, висок, умерен) узимајући у обзир утицај на поверљивост, доступност, безбедност, интегритет и/или отпорност 5G мреже, као и обим утицаја у смислу корисника, трајања, броја базних станица које су погођене, осетљивост информација које су измењене или којима се приступило и друге утицаје;

– Идентификацију потенцијалних претњи, анализа рањивости и процена ризика везаних за кључне компоненте 5G мреже који могу утицати на безбедност и функционалност 5G мреже, укључујући ризике од сајбер напада, физичке претње, технолошке нестабилности и слично;

– Процену ризика добављача 5G опреме која припада некој од кључних компоненти 5G мреже који учествују у изградњи, одржавању или управљању 5G мрежом, укључујући и добављаче услуга управљања мрежом која треба да укључи безбедносне аспекте опреме и услуга које добављач пружа, потенцијалне претње по интегритет 5G мреже, ризике од неовлашћеног приступа или злонамерних активности и друто;

– Процену степена диверзификације добављача 5G опреме која припада некој од кључних компоненти 5G мреже;

– Предложене мере за елиминисање или ублажавање идентификованих претњи, рањивости и ризика, укључујући али не ограничавајући се на мере предвиђене овом уредбом;

– План за спровођење предложених мера.

Елементи које процена ризика оператора 5G мреже из става 2. овог члана треба да садржи су детаљније наведени у Прилогу 1, који чини саставни део ове уредбе.

За процену ризика добављача 5G опреме оператор 5G мреже прикупља податке и информације од добављача 5G опреме, уз поштовање поверљивости података. Добављач 5G опреме је дужан да достави податке оператору за потребе израде појединачне процене ризика оператора.

Оператори 5G мреже су дужни да своје процене ризика ажурирају најмање једном у две године или у року од шест месеци од измене у некој од кључних компоненти 5G мреже које су оцењене критичним степеном осетљивости или на захтев министарства, посебно у случају угрожености националне безбедности и одбране, и у том случају рок за израду не може бити краћи од шест месеци.

Оператори 5G мреже су одговорни за процену ризика коју спроводе и за усклађеност са обавезама утврђеним у овом члану.

Процена ризика од стране добављача 5G опреме

Члан 8.

Добављачи 5G опреме која припада некој од кључних компоненти 5G мреже који су присутни или који планирају улазак на тржиште Републике Србије су дужни да израде сопствену процену ризика и рањивости опреме и софтвера, као и процену техничких аспеката безбедности опреме и софтвера и да предложе мере за елиминисање или ублажавање идентификованих ризика и рањивости.

Елементи које процена ризика добављача 5G опреме из става 1. овог члана треба да садржи дати су у Прилогу 2, који чини саставни део ове уредбе.

Добављачи 5G опреме достављају иницијалну анализу ризика Министарству најкасније у року од девет месеци од ступања на снагу ове уредбе.

Добављачи 5G опреме су дужни да своје процене ризика ажурирају најмање једном у две године или на захтев министарства и у том случају рок за израду не може бити краћи од шест месеци.

У складу са одредбама члана 7. став 4. ове уредбе добављачи 5G опреме достављају информације и податке операторима 5G мреже који користе њихову опрему, хардвер, софтвер и/или помоћне услуге које су наведене као кључне компоненте 5G мреже за потребе израде процене ризика од стране оператора 5G мреже.

Добављачи 5G опреме су одговорни за процену ризика коју спроводе и за усклађеност са обавезама утврђеним у овом члану.

Процена ризика добављача 5G опреме

Члан 9.

У оквиру националне процене ризика из члана 6. ове уредбе, Министарство спроводи процену ризика добављача 5G опреме која припада некој од кључних компоненти 5G мреже и утврђује мере за превазилажење или ублажавање ових ризика, у сарадњи са органима из члана 6. став 3. ове уредбе.

Процена ризика добављача укључује процену техничких, технолошких и безбедносних фактора који укључују:

1) процену техничких аспеката безбедности опреме и софтвера добављача, узимајући у обзир потенцијалне рањивости у дизајну, кодирању и интеграцији опреме у 5G мрежу;

2) способност добављача да обезбеди континуирано снабдевање и могућност контроле сопственог ланца снабдевања (под-добављача);

3) постојање претходних инцидената добављача у области информационе безбедности у Републици Србији и

4) карактеристике власничке структуре добављача и повезаност добављача са владом матичне државе која ствара вероватноћу мешања те државе у

пословање добављача, укључујући и могућност да утиче на локацију производње добављача.

На основу процене и примене свих критеријума из става 2. овог члана и стручног мишљења органа из члана 6. став 3. ове уредбе, могу се применити следеће мере, у зависности од степена осетљивости кључних компонената 5G мреже:

– ограничење или забрана употребе опреме и услуга добављача у кључним компонентама 5G мреже које су означене са критичним степеном осетљивости и само ако се сврха не може постићи неком од ниже прописаних мера;

– примена додатних безбедносних провера и надзора пре употребе 5G опреме добављача у кључним компонентама 5G мреже;

– захтев да добављач испуњава стандарде у складу са прописима који уређују област електронских комуникација и област информационе безбедности;

– успостављање обавезне сертификације за 5G опрему и софтвер, при чему сертификацију могу спроводити независна тела, пре интеграције опреме у 5G мрежу;

– спровођење редовне ревизије од стране овлашћене независне организације, о трошку добављача, како би се проценила усклађеност опреме и услуга добављача са безбедносним стандардима.

У случају примене мере из става 3. тачка 1. овог члана у оквиру националне процене ризика биће дефинисан временски период у ком је потребно ограничити или заменити опрему и/или услуге, при чему ће се водити рачуна пре свега о безбедносним ризицима задржавања опреме, као и техничким и економским потешкоћама у спровођењу мере.

Временски период из става 4. овог члана не може бити краћи од две и не може бити дужи од пет година.

Процена ризика добављача услуга управљања мрежом

Члан 10.

Оператори 5G мреже су дужни да идентификују, процене и управљају ризицима који произилазе из коришћења услуга које пружају добављачи услуга управљања мрежом (Managed Service Providers – MSP), укључујући и добављаче услуга управљања безбедношћу (Managed Security Service Providers – MSSP) које се односе на одржавање, управљање и надзор мрежне инфраструктуре, као и пружање безбедносних решења и подршке у оквиру кључних компоненти 5G мреже.

Потенцијални ризици коришћења услуга добављача услуга управљања укључују:

– ризике од неовлашћеног приступа и промене мрежне конфигурације;

– ризике од сајбер напада који могу угрозити безбедност мреже и података;

– ризике од неадекватне безбедности у процесу пружања услуга управљања мрежом, што може утицати на доступност и интегритет мреже;

– ризике који произилазе из зависности од спољних добављача и могућности прекида услуга које они пружају.

Оператори 5G мреже су дужни да примењују следеће мере у циљу управљања ризицима који се односе на добављаче услуга управљања мрежом:

– спроводе стални мониторинг безбедносних активности добављача услуга управљања мрежом, како би идентификовали и благовремено реаговали на потенцијалне претње;

– обезбеде да добављачи услуга управљања мрежом који пружају услуге на кључним компонентама 5G мреже испуњавају прописане безбедносне стандарде, укључујући захтеве за контролу приступа, управљање подацима и заштиту од сајбер напада.

– осигуравају да добављачи услуга управљања мрежом примењују техничке мере које укључују контролу приступа, аутентификацију и ауторизацију, као и евидентирање приступа и активности;

– успоставе уговорне обавезе са добављачима услуга управљања мрежом који укључују конкретне одредбе о безбедности и управљању ризицима, укључујући обавезу редовног извештавања о безбедносним инцидентима и спровођењу мера заштите.

Оператори 5G мреже су дужни да у оквиру процене ризика оператора из члана 7. ове уредбе опишу идентификоване ризике који су повезани са добављачима услуга управљања мрежом, као и мере које су предузете за ублажавање или елиминисање идентификованих ризика.

Процена степена диверзификације добављача 5G мреже

Члан 11.

Оператори 5G мреже су дужни да спроводе стратегију диверзификације добављача 5G опреме која припада некој од кључних компоненти 5G мреже како би се избегла зависност свих кључних компоненти 5G мреже од појединачног добављача.

За ове сврхе сматра се да добављачи 5G опреме нису различити ако су у власништву или под контролом истог субјекта.

Оператори 5G мреже су дужни да у оквиру процене ризика оператора из члана 7. ове уредбе наведу све постојеће добављаче 5G опреме за све кључне компоненте 5G мреже, као и добављаче од којих планирају да набављају кључне компоненте 5G мреже у наредне две године.

Ако се у националној процени ризика утврди да су у 5G мрежи једног оператора све кључне компоненте 5G мреже означене са критичним степеном осетљивости од истог добављача 5G опреме може се одредити и мера увођења најмање још једног добављача 5G опреме, под условом да је на тај начин омогућена интероперабилност 5G опреме различитих добављача.

Уколико није могуће обезбедити интероперабилност 5G опреме различитих добављача онда се за кључне компоненте 5G мреже означене са критичним

степеном осетљивости може одредити нека од мера из члана 9. став 3. ове уредбе.

Министарство ће у оквиру националне процене ризика дефинисати временски период за диверзификацију добављача 5G опреме која захтева ограничење или замену опреме и/или услуга, при чему ће се водити рачуна пре свега о безбедносним ризицима задржавања опреме, као и техничким и економским потешкоћама у спровођењу мере.

Временски период из става 6. овог члана не може бити краћи од две и не може бити дужи од пет година.

Остале мере за смањење безбедносних ризика

Члан 12.

Оператори 5G мреже су дужни да за утврђене претње, рањивости и ризике у оквиру процене ризика оператора из члана 7. ове уредбе, предложе техничке мере које су у складу са утврђеним претњама, рањивостима и ризицима који се односе на безбедност 5G мреже и које подразумевају да:

– примене мере безбедносне заштите из релевантних стандарда за 5G мреже (3GPP), у сарадњи са добављачима;

– примене најбоље праксе и политике за контролу приступа кључним компонентама 5G мреже (посебно приступа трећих страна) који треба да обезбеде довољну контролу приступа, одговарајуће механизме за праћење приступа и процедуре за управљање ризицима који проистичу из интеракције са трећим странама;

– имплементирају одговарајуће алате и процесе за одржавање интегритета софтвера у кључним компонентама 5G мреже;

– захтевају од својих добављача у процесу набавке опреме која се односи на кључне компоненте 5G мреже одговарајући ниво безбедносних стандарда.

Надлежно тело за праћење и контролу примене мера из става 1. овог члана је Регулатор. Оператори 5G мреже су обавезни да на сваке две године достављају Регулатору извештаје о примени мера из става 1. овог члана.

Подршка мерама

Члан 13.

Подршка стратешким и техничким мерама које су предвиђене овом уредбом може да обухвати:

1) техничку подршку и размену информација - оператори и надлежни органи сарађују ради пружања техничке подршке, размене информација и најбољих пракси, у циљу осигурања безбедности 5G мрежа;

2) развој вештина и ресурса – државни органи, у сарадњи са академском заједницом и индустријом, обезбеђују програме обуке и развоја вештина за техничке стручњаке и особље задужено за управљање и надзор 5G мрежа, како би се повећали капацитети за процену и управљање ризицима;

3) тестирање и сертификацију – оператори и произвођачи опреме обавезни су да се придржавају програма тестирања и сертификације који су усклађени са европским и међународним стандардима, са циљем да се осигурају техничка исправност и безбедност кључних компоненти 5G мрежа;

4) међународну сарадњу – надлежни органи активно учествују у међународним иницијативама и сарађују са земљама Европске уније, као и другим релевантним актерима, ради унапређења безбедности 5G мрежа и координације активности у области информационе безбедности;

5) едукацију и подизање свести – органи надлежни за електронске комуникације или информациону безбедност организују кампање и активности усмерене на подизање свести јавности и привредних субјеката о важности безбедности 5G мрежа и мера заштите;

6) мониторинг и извештавање – органи надлежни за електронске комуникације или информациону безбедност редовно прате спровођење мера подршке.

Ступање на снагу

Члан 14.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-1720/2025-2

У Београду, 27. фебруара 2025. године

Влада

Председник,

Милош Вучевић, с.р.

ПРИЛОГ 1

САДРЖАЈ ПРОЦЕНЕ РИЗИКА ОД СТРАНЕ ОПЕРАТОРА 5G МРЕЖЕ

Основни елементи процене ризика од стране оператора 5G мреже обухватају:

1. Процена осетљивости кључних компоненти 5G мреже и њихова категоризација

Оператори могу да идентификују и додатне елементе и функције које представљају кључне компоненте 5G мреже у односу на списак који је дат у оквиру члана 5. став. 1 ове уредбе.

Сваки идентификовани елемент и функција у оквиру кључних компоненти 5G мреже треба да се процени са аспекта безбедносног ризика који се односи на доступност мрежних функција (како би се осигурао континуираног рада мреже), поверљивост информација (како би се заштитиле осетљиве информације), сигурност (заштита од неовлашћених приступа) и отпорност 5G мреже (способност опоравка од инцидената).

Категоризација осетљивости сваког елемента и функције у оквиру кључних компоненти 5G мреже на основу степена утицаја треба да обухвати следеће нивое осетљивости:

– Критичан: Ова категорија обухвата елементе и функције чије компромитовање може изазвати:

– Знатан прекид у раду 5G мреже који погађа велики број корисника;

– Утицај на велики број базних станица или целокупне регионалне мреже;

– Компромитовање поверљивих информација високог степена значаја.

– Висок: Ова категорија укључује елементе и функције чије компромитовање може:

– Значајно умањити функционалност појединачних сервиса или мреже у специфичним областима;

– Утицати на осетљиве информације које су важне, али не критичне;

– Захтевати брзу интервенцију ради ублажавања последица, али без дуготрајног утицаја на мрежу у целини.

– Умерен: Ова категорија укључује елементе и функције чије компромитовање има:

– Локализован и ограничен утицај на мањи број корисника или базних станица;

– Минималан или привремен утицај на поверљивост или доступност информација.

За одређивање степена осетљивости користи се матрица ризика која укршта два кључна фактора:

– Вероватноћа претње (ниска, средња, висока);

– Последице у случају компромитовања: (ниске, умерене, критичне).

2. Идентификацију претњи и анализа рањивости везаних за кључне компоненте 5G мреже

Оператори треба да идентификују све потенцијалне претње које могу утицати на кључне компоненте 5G мреже. Ове претње најчешће укључују:

– Сајбер претње као што су DDoS напади, неовлашћени приступ или манипулација подацима;

– Физичке претње као што су природне катастрофе, вандализам или намерно оштећење инфраструктуре које могу нарушити стабилност мреже;

– Унутрашње претње које потичу од запослених, трећих лица или партнера, укључујући могуће злоупотребе или немар;

– Претње повезане са добављачима које произилазе из процене ризика добављача у складу са тачком 3. овог прилога;

– Претње из ланца снабдевања односе се на претње које настају током различитих фаза набавке, производње, транспорта и интеграције компоненти у мрежу.

Анализа рањивости треба да идентификује све слабости у мрежи које могу бити искоришћене од стране идентификованих претњи које могу укључивати:

– техничке рањивости које могу произилазити из неажурних или застарелих софтверских пакета, неефикасног шифровања или слабих алгоритама, слабих механизама аутентификације и сл.;

– оперативне рањивости које могу да настану услед недостатка процедура за управљање инцидентима, лоше конфигурације система, недостатка обуке особља и сл.;

– организационе рањивости које произлазе из неуспелог спровођења безбедносних политика, лоше дефинисаних процеса итд.

Све идентификоване претње треба да буду систематизоване према њиховој вероватноћи настанка и могућем утицају на функционисање 5G мреже.

Вероватноћа настанка претње може бити класификована као ниска вероватноћа (ретки случајеви), средња вероватноћа (могуће, али не уобичајено) или висока вероватноћа (веома вероватно) узимајући у обзир факторе као што су историјски подаци о сличним претњама, ефикасност постојећих безбедносних мера и сл.

Процена потенцијалног утицаја на функционисање 5G мреже се врши узимајући у обзир како идентификована претња може утицати на доступност мрежних функција, поверљивост информација, сигурност и отпорност 5G мреже, а процене се класификују да имају ниски утицај (локализоване и брзо решиве последице), средњи утицај (делимично угрожавање кључних функција) или високи утицај (велике и дуготрајне последице које угрожавају интегритет целе мреже).

За систематизовање претњи користи се матрица ризика која укршта два кључна фактора:

– Вероватноћа настанка (ниска, средња, висока);

– Утицај на функционисање 5G мреже (низак, средњи, висок).

3. Процена ризика добављача 5G опреме, укључујући и процену ризика добављача услуга управљања мрежом

Процене ризика добављача 5G опреме која припада некој од кључних компоненти 5G мреже, укључујући и процену ризика добављача услуга управљања мрежом треба да садржи:

а) Идентификацију добављача:

Направити списак свих постојећих добављача кључних компоненти 5G мреже и добављача услуга управљања мрежом, као и добављача од којих се планира набавка опреме и/или услуга за кључне компоненте 5G мреже у наредне две године, који укључују:

– Тип опреме или услуге коју добављач пружа;

– Локације на којима се користи опрема или услуга датог добављача.

б) Процену безбедносног профила добављача:

– Испитати безбедносне политике добављача, укључујући мере заштите података, контроле приступа и процедуре за одговор на инциденте;

– Проценити транспарентност добављача у вези са пореклом компоненти и софтвера који се користе у 5G мрежи;

– Проверити компатибилност са националним и европским безбедносним стандардима (нпр. ISO 27001);

– Описати историјат безбедносних инцидената у које је добављач укључен уколико постоји;

– Историја претњи или рањивости у испорученој опреми или услугама;

– Оценити спремност на сарадњу у области информационе безбедности.

в) Техничку процену опреме и услуга

– Спровести техничко тестирање опреме и софтвера на потенцијалне рањивости, укључујући анализу кода и проверу могућих „задњих врата" (backdoors) или

– Проценити усклађеност са међународним техничким стандардима и примену најбољих пракси у дизајну и развоју.

4. Диверзификација добављача

Проценити зависност од добављача за сваку од кључних компоненти 5G мреже на основу параметара као што су број различитих добављача за исте елементе и функције које припадају кључним компонентама 5G мреже и географска и технолошка разноврсност.

5. Предложене мере за елиминисање или ублажавање идентификованих претњи, рањивости и ризика

На основу идентификованих претњи, рањивости и процене ризика, оператори 5G мреже предлажу мере које укључују али се не ограничавају на:

– Техничке мере које се односе на употребу шифровања, ограничење приступа, сегментацију мреже и мултифакторску аутентификацију, редовна ажурирања софтвера, успостављање система за праћење активности добављача у реалном времену, уз логовање свих приступа;

– Организационе мере укључујући обуку особља, процедуре за управљање инцидентима итд.;

– Укључивање безбедносних клаузула у уговоре са добављачима, укључујући извештавање о безбедносним мерама и инцидентима, пружање подршке у случају инцидената и сл.;

– Мере које се односе на диверзификацију добављача и с тим у вези имплементацију стандарда који омогућавају интероперабилност различитих решења.

За све предложене мере оператори достављају и план за спровођење.

Поред наведеног оператори могу користити и стандардизоване методологије као што су NIST SP 800-30 и/или ISO/IEC 27005 за идентификовање претњи, анализу рањивости, утврђивање ризика и предлог одговарајућих мера за њихово елиминисање или ублажавање.

Сви подаци и анализе који се користе у процени ризика морају бити образложени и документовани.

ПРИЛОГ 2

САДРЖАЈ ПРОЦЕНЕ РИЗИКА ОД СТРАНЕ ДОБАВЉАЧА 5G ОПРЕМЕ

Основни елементи процене ризика од стране добављача 5G опреме обухватају:

1. Идентификација и процена ризика и рањивости који укључују:

– процену технолошких ризика који су повезани са новим и напредним технологијама, као што су нови протоколи, архитектуре и стандарди који се користе у 5G мрежама. Ово укључује и процену потенцијалних рањивости у дизајну, кодирању и интеграцији опреме.

– процену безбедносних ризика који обухватају анализу потенцијалних утицаја на безбедност, као што су рањивости у опреми, напади на мрежну инфраструктуру и могући утицај злоупотребе података, постојање претходних инцидената добављача у области информационе безбедности у Републици Србији.

– процену оперативних ризика који се могу јавити током инсталације, конфигурације, тестирања и одржавања 5G опреме.

– процену ризика у вези са снабдевањем и ланцем снабдевања који се односе на кашњења у снабдевању, неиспуњавање стандарда или други проблеми са добављачима.

Добављачи 5G опреме могу да идентификују и друге ризике и рањивости.

Квантификација ризика помоћу матрице ризика омогућава систематски приступ у процени ризика и рањивости, чиме се добија јаснија слика о тежини и вероватноћи одређених ризика.

Матрица ризика треба да комбинује два параметра:

1. Вероватноћа појаве ризика (висока, средња, ниска).

2. Утицај ризика (високи, средњи, ниски).

Поред наведеног добављачи могу користити и стандардизоване методологије као што су NIST SP 800-30 и/или ISO/IEC 27005 за идентификовање и процену ризика и рањивости и предлог одговарајућих мера за њихово елиминисање или ублажавање.

2. Техничка процена безбедности опреме и софтвера добављача:

Подразумева процену техничких аспеката безбедности опреме и софтвера добављача, узимајући у обзир потенцијалне рањивости у дизајну, кодирању, интеграцији и управљању опремом кроз:

– процену да ли опрема користи сигурне методологије у дизајну, као што су примена принципа „Security by Design” или „Privacy by Design”, као и техничке контроле за спречавање неовлашћеног приступа;

– процену безбедности софтвера са фокусом на познате рањивости и примена најбољих пракси за безбедно кодирање;

– примену процедура тестирања безбедности и укључивање независних тела за проверу интегритета система;

– примену процедура за јачање интегритета софтвера, ажурирање и управљање ажурирањем софтвера током животног века компоненте;

– оцењивање способности опреме да ради у сложеним мрежним окружењима без угрожавања других делова мреже;

– процену доступности транспарентних и сигурних функција за управљање и надзор, укључујући спречавање неовлашћеног приступа.

3. Предложене мере за елиминисање или ублажавање идентификованих ризика и рањивости:

– анализа усклађености са стандардима која осигурава да опрема буде у складу са релевантним стандардима;

– процена утицаја на инфраструктуру која омогућава процену како нова опрема може утицати на постојеће мреже и инфраструктуру, што је кључно за идентификацију и минимизирање ризика који се односе на интеграцију нових технологија и одржавање стабилности и сигурности постојећих мрежа;

– стратегија за осигурање квалитета и планови за тестирање и верификацију како би се омогућило откривање потенцијалних проблема у раним фазама и смањиле могућности дефеката и грешака у опреми;

– стратегије за праћење и идентификовање нових ризика које подразумевају стратешко опредељење за праћење током читавог животног века опреме;

– сарадња са операторима 5G мреже у спровођењу пенетрацијских тестова и/или спровођење пенетрацијских тестова у тестном окружењу и транспарентна подела информација са операторима о рањивостима које су откривене у пенетрацијским тестовима спроведеним у другим државама;

– стратегије за минимизацију ризика у ланцу снабдевања која обухвата управљање ризицима који се јављају у ланцу снабдевања, као што су кашњења, неиспуњавање стандарда или поремећаји у снабдевању.

Добављачи могу да предложе и друге мере за елиминисање или ублажавање идентификованих ризика и рањивости.

За све предложене мере добављачи 5G опреме достављају и план за спровођење.

Сви подаци и анализе који се користе у процени ризика морају бити образложени и документовани.